REMARKS

Claims 1, 3-18, 20-29, 31 and 32 are currently pending in the subject application and are presently under consideration. Claims 1, 18, 27, 28 and 31 have been amended as shown on pages 2- 6 of the Reply. The below comments present in greater detail distinctive features of applicants' claimed invention over the cited art that were conveyed to the Examiner over the telephone on February 14, 2008.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1, 3-16, 28-29 and 31-32 Under 35 U.S.C. §101

Claims 1, 3-16, 28-29 and 31-32 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Withdrawal of this rejection is requested for the following reasons. Independent claims 1, 28 and 31 have been amended herein, and in view of this, the rejection is believed to be moot and should be withdrawn.

II. Rejection of Claims 1, 6-15 and 17 Under 35 U.S.C. §103(a)

Claims 1, 6-15 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (U.S. 6,986,050 B2) further in view of Bathrick, *et al* (U.S. 5,825,300). Withdrawal of this rejection is requested for the following reasons. Brainard, Hyppopen and Bathrick *et al*., individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. In particular, independent claim 1 recites *a wrapper that packages credentials associated with resources of a service**; and a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials,** the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials*. Brainard, Hypponen and Bathrick, individually or in combination, fail to teach or suggest such novel features recited by the subject claims.

Brainard relates to an architecture that secures access to network resources, while providing a smooth migration path from legacy authentication and authorization methods to a

public key infrastructure. At page 6 of the Final Office Action, the Examiner concedes that Brainard does not teach such novel features. The Examiner attempts to compensate for the aforementioned deficiencies of Brainard with Hypponen and Bathrick *et al.*

Hypponen discloses a method of securing data stored in an electronic device comprising encrypting the data using a cryptographic key. At the cited portions, Hypponen discloses a system that allows a user to make use of a long passphrase having sufficient entropy to ensure adequate security, and at the same time a relatively short password for frequent use. The passphrase authenticates the user when the user logs on, and allows access to the data. Subsequently, when a user returns to the system after period of idleness, the system allows the user to enter a password to access the data. Thus, the password and the passphrase are the credentials that facilitate access to the resources on the device. A cryptographic key is generated from the passphrase, and is used to encrypt and decrypt data stored on the device. Alternatively, Hypponen discloses the cryptographic key being generated separately and the key being encrypted using the passphase or using a second key derived using the passphase. Thus, Hypponen discloses a passphrase that is used to generate/access a cryptographic key that facilitates in encrypting and decrypting data stored in the device, where the passphrase is employed to access to the device resources. On the contrary, the claimed invention generates a passphrase, a cryptographic wrapping key is generated from the pass-phase and this key is employed to *generate the wrapper* in which the credentials are wrapped. The passphrase is employed to facilitate access to the credentials, where the credentials are employed to access resources of the service. Thus, Hypponen is silent regarding ***a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials*** as recited by the subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. At the cited portions, Bathrick *et al.* discloses a certifying authority that generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network. However, nowhere does Bathrick *et al.* teach ***a pass phrase employed in connection with generation of the wrapper via a cryptographic wrapping key*** as taught by applicants' subject claims.

In view of the above, Brainard, Hyppopen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is respectfully submitted that this rejection be withdrawn with respect to independent claim 1(and the claims that depend there from).

III. Rejection of Claim 16 Under 35 U.S.C. §103(a)

Claim 16 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (U.S. 6,986,050 B2) further in view of Bathrick, *et al* (U.S. 5,825,300) further in view of Kay, *et al.* (U.S. 6,993,555 B2). Withdrawal of this rejection is requested for the following reasons. Claim 16 depends from independent claim 1. As discussed *supra*, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claim. Kay *et al.* relates to a system for autonomously processing requests from remotely located users, using an instant messaging protocol, and does not make up for the deficiencies of Brainard, Hypponen, and Bathrick *et al.* with respect to independent claim 1. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 1(from which claim 16 depends) be withdrawn.

IV. Rejection of Claims 3-5 Under 35 U.S.C. §103(a)

Claims 3-5 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (U.S. 6,986,050 B2) further in view of Bathrick, *et al* (U.S. 5,825,300) further in view of Rahman, *et al.* (U.S. 7,114,080 B2). Withdrawal of this rejection is requested for the following reasons. Claims 3-5 depend from independent claim 1. As discussed *supra*, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claim. Rahman *et al.* relates to a system that employs multiple computers outside a firewall and a password scheme that includes a one-time password and has biometric features, and does not make up for the deficiencies of Brainard, Hypponen, and Bathrick *et al.* with respect to independent claim 1. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 1(from which claims 3-5 depend from) be withdrawn.

V. Rejection of Claims 18 and 20 Under 35 U.S.C. §103(a)

Claims 18 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Epstein, *et al.* (U.S. 2002/0124064 A1) in view of Hardy, *et al.* (U.S. 5,222,135) further in view of Bathrick, *et al.* (U.S. 5,825,300). Withdrawal of this rejection is requested for the following reasons. Epstein *et al.*, Hardy *et al.* and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. Amended independent claim 18 recites *a method to facilitate a security connection between entities, comprising: generating a strong password; generating a pass-phrase;* ***wrapping the password cryptographically via the pass-phrase; storing the wrapped password in an executable, wherein the pass-phrase facilitates in unlocking the wrapper;*** *and transmitting the executable and the pass-phrase to a system via different communications mediums.* Epstein *et al.*, Hardy *et al.* and Bathrick *et al.* are silent regarding such novel features.

Epstein *et al.* relates to a method to control a network through distributed control points. At page 10 of the Final Office Action, the Examiner contends that Epstein *et al.* teaches such novel features. Applicants' representative avers to the contrary. In accordance with the claimed invention, the system generates a pass phrase, which is employed to generate a cryptographic wrapping key. The wrapping key is then employed to cryptographically wrap or insulate the password in the wrapper or package. After the password has been placed in the wrapper, the passphrase facilitates in unlocking the wrapper to retrieve the password. At the cited portions, Epstein *et al.* discloses a pass phrase that has the one time key encoded within it. A control point is activated using the pass phrase. A new connection from the activated control point is received by using the one time key extracted from the pass phrase. Nowhere does Epstein *et al.* teach using the pass phrase to unlock the wrapper to access the password, and hence is silent regarding ***wrapping the password cryptographically via the pass-phrase, wherein the pass-phrase facilitates in unlocking the wrapper*** as recited by the subject claims. The Examiner attempts to compensate for the aforementioned deficiencies of Epstein *et al.* with Hardy *et al.* and Bathrick *et al.*

Hardy *et al.* relates to a method for controlling the use of a data processing workstation by password. At the cited portions, Hardy *et al.* discloses storing an encrypted password in an

executable and transmitting it. The password however, is not cryptographically wrapped via the pass phrase. Hence, Hardy *et al.* is silent regarding ***wrapping the password cryptographically via the pass-phrase, wherein the pass-phrase facilitates in unlocking the wrapper;*** as recited by the subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. Bathrick *et al.* does not teach ***wrapping the password cryptographically via the pass-phrase, wherein the pass-phrase facilitates in unlocking the wrapper*** as recited by the subject claims.

In view of the above, Epstein *et al.*, Hardy *et al.* and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is respectfully submitted that this rejection be withdrawn with respect to independent claim 18 (and the claims that depend there from).

VI. Rejection of Claims 21-26 Under 35 U.S.C. §103(a)

Claims 21 and 26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Epstein, *et al.* in view of Hardy, *et al.* further in view of Bathrick, *et al.* further in view of Brainard (SecurSight: Architecture for Secure Information). Withdrawal of this rejection is requested for the following reasons. Claims 21-26 depend from independent claim 18. As discussed *supra*, Epstein *et al.*, Hardy *et al.* and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claim. Brainard relates to an architecture that secures access to network resources, while providing a smooth migration path from legacy authentication and authorization methods to a public key infrastructure, and does not make up for the deficiencies of Epstein *et al*, Hardy *et al.* and Bathrick *et al.* with respect to independent claim 18. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 18 (from which claims 21-26 depend from) be withdrawn.

VII. Rejection of Claims 27-29 and 31-32 Under 35 U.S.C. §103(a)

Claims 27-29 and 31-32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Rahman, *et al* (U.S. 7,114,080 B2) in view of Nemovicher (U.S. 2002/0007453 A1). Withdrawal of this rejection is requested for the following reasons. Rahman *et al.*, and

Nemovicher, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. Amended independent claim 27 recites *computer implemented means for generating a password;* ***computer implemented means for generating a pass-phrase****; computer implemented means for generating a package of credentials,* ***wherein the credentials are packaged by wrapping them cryptographically; computer implemented means for storing the password separate from the package; computer implemented means for locking the package with the pass-phrase****; and computer implemented means for transmitting the package and the pass-phrase to a system via different communications mediums.* Independent claim 31 recites similar features. Rahman *et al.*, and Nemovicher are silent regarding such novel features.

Rahman *et al.* relates to a system that uses biometric features combined with a one-time password to generate cryptographic keys that are used for secure communication, authentication of remote users and accessing secured files. At page 14 of the Final Office Action, the Examiner concedes that Rahman *et al.* does not teach a pass phrase employed in connection with generation of cryptographic wrapping key, the pass phrase distributed separately from the credentials. The Examiner attempts to compensate for the aforementioned deficiencies of Rahman *et al.* with Nemovicher.

Nemovicher relates to a client server system for sending and receiving secure e-mail transmissions that are date stamped, virus scanned and authenticated at a centralized server. At the cited portions, Nemovicher discloses an e-mail message from a sender, along with a digital signature for authentication, being received by a server, the server decrypts the message, verifies it and adds another digital signature, encrypts the message with a one-time random key, and re-transmitts the secure message to a recipient who does not subscribe to the service. The one time random key is encrypted and packaged with the encrypted message form, a public key generated from a pass phrase (or password) taken from the saved sender e-mail message and both digital signatures, the package is attached to an e-mail message and sent to the recipient. The recipient can open the received package using the pass phrase (or password) obtained through separate communication channels from the sender. The system of Nemovitch packages the credentials and sends it to the recipient who uses the pass phrase to open the package, get the credentials and

view the message. However, Nemovitch is silent regarding means for storing the password, and for locking the package with a pass phrase separate from the password. Further, Nemovitch discloses a recipient who subscribes to the service, receiving the package and opening it with the encrypted private key. In that embodiment, the pass phrase is not transmitted via different communication mediums. Thus, Nemovitch does not teach *means for generating a package of credentials, wherein* ***the credentials are packaged by wrapping them cryptographically, computer implemented means for storing the password separate from the package; computer implemented means for locking the package with the pass-phrase*** as recited by the subject claims.

In view of the above, it is clear that Rahman *et al.*, and Nemovicher, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP319US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731